An Analysis of Security and Privacy of Emails in e-Mentoring

Liam Caffery [1], Sarah Stewart [1,2] and Anthony C Smith [1]

1. Centre for Online Health, University of Queensland, Australia
2. School of Midwifery, Otago Polytechnic, Dunedin, New Zealand

Introduction

Email is an effective way of implementing an e-mentoring program for health care workers because of the flexibility of asynchronous communication.[1] When the content of an email is sensitive or identifies a patient it is considered best-practice to encrypt the email to maintain patient confidentiality.

> Emails are most often sent across a public network — the Internet — in plain text. Further, emails sent or received using an employer's email system can be both legally and technically read by the employer.

Box 1: The security risk of email

Aim

The aim of this study was to determine the level of security and privacy needed by an email system used in e-mentoring.

Methods

We ran a 12- month multi-centre, multi-disciplinary e-mentoring pilot study for clinicians involved in the delivery of residential home care nursing, midwifery and allied health therapies. During the pilot a total of 108 emails were sent.

For the study, we used a secure, web-based email application as the means of communication between mentor and mentee. The application forces all correspondence to be encrypted using

> Secure Socket Layer and Transport Layer Security are standardised methods of Public Key Infrastructure (PKI): a form of cryptography that prevents the unauthorised reading of email's content.

Box 2: Standard methods of Public Key Infrastructure

We devised an eight-point security scale to rate the security and privacy sensitivity of emails between a mentor and mentee. (Table 1) We analysed the content of actual emails for the pilot project and assigned a security classification score to each of the emails.

Table 1: The security scale, description and example used to classify emails in our study.

Score	Description
1	Email contains patient identifiable content where the confidentiality of the patient is breached by identifying medical condition or treatment.
2	Email contains patient identifiable information but does not disclose medical condition or treatment
3	Email identifies staff member involved in a practice that places them or other staff member at professional risk.
4	Email identifies staff member and divulges possible stigmatising information about themselves or other staff member.
5	Email identifies staff member and divulges information that could embarrass themselves or other staff member.
6	Email identifies staff member and describes a clinical event or professional event.
7	Email identifies staff member and divulges personal information about themselves or other staff member.
8	None of the above

Results

The mean security classification score was 6.30. (n=108, SD= 1.09). The range of security classification scores was 3 – 8 and the interquartile range (IQR) was 6- 7. There were no emails for either security classification scores 1 or 2 — meaning no patient identifiable data was divulged in any correspondence during the study period. (Figure 1)

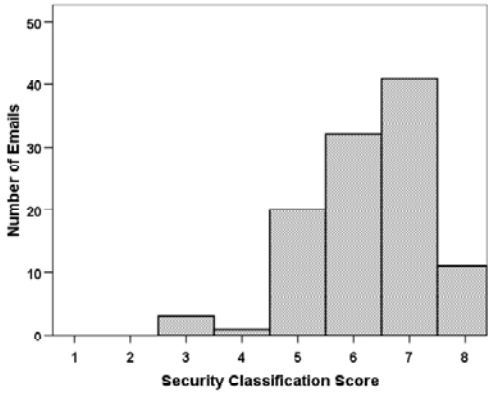

Figure 1: Histogram of security scores for the pilot study

Conclusion

The study shows that disclosure of patient identifiable data is not integral to e-mentoring. Hence, email systems used for e-mentoring do not need to comply with encryption techniques to meet legal requirements. We also showed that staff involved in an e-mentoring relationship will divulge sensitive or stigmatising information about themselves, colleagues or employer. Hence, the use of employer's email system is not recommended for e-mentoring as scrutiny of content may stifle correspondence on sensitive issues — possibly reducing the effectiveness of mentoring.

HMMU August'07 ss 1301Caffery/Smith P2_ai